

CLAIMS

Sub
a1

1. A method for configuration management for a computing device,
2 comprising the steps of:
4 providing available software to said computing device through an
6 interface;
8 determining whether or not resident software stored in a storage device
associated with said computing device is authenticated; and
loading said available software into said storage device if said resident
software has not been authenticated.
2. The method of claim 1 further comprising the steps of:
2 determining whether or not said available software is authenticated;
4 rejecting said available software if said resident software is authenticated
and said available software is not authenticated; and
6 loading said available software if said resident software is authenticated
and said available software is authenticated.
3. The method of claim 1 wherein the step of determining whether
2 or not said resident software is authenticated comprises the steps of:
4 determining whether or not an authentication flag has been set;
6 wherein said resident software is determined to be authenticated if said
authentication flag has been set; otherwise
said resident software is determined to be unauthenticated.
4. The method of claim 3 wherein said authentication flag is set
2 when authenticated software has been loaded onto said computing device.
5. The method of claim 3 wherein said authentication flag is set by a
2 service technician.
6. The method of claim 1 wherein the step of determining whether
2 or not said resident software is authenticated comprises the step of performing
a direct authentication procedure on said resident software.
7. The method of claim 6 wherein said direct authentication
2 procedure comprises performing a cyclic redundancy check.

009001 925530

14. The apparatus of claim 9 wherein said processor is further for performing a direct authentication procedure on said resident software to determine whether or not said resident software is authenticated.

$$\begin{array}{ccccccc} \{a_1, \dots, a_n\} & \{b_1, \dots, b_m\} & \{c_1, \dots, c_k\} & \{d_1, \dots, d_l\} & \{e_1, \dots, e_p\} & \{f_1, \dots, f_q\} & \{g_1, \dots, g_r\} \\ \{h_1, \dots, h_s\} & \{i_1, \dots, i_t\} & \{j_1, \dots, j_u\} & \{k_1, \dots, k_v\} & \{l_1, \dots, l_w\} & \{m_1, \dots, m_x\} & \{n_1, \dots, n_y\} \\ \{o_1, \dots, o_z\} & \{p_1, \dots, p_{10}\} & \{q_1, \dots, q_{10}\} & \{r_1, \dots, r_{10}\} & \{s_1, \dots, s_{10}\} & \{t_1, \dots, t_{10}\} & \{u_1, \dots, u_{10}\} \end{array}$$

16. The apparatus of claim 14 wherein said direct authentication
2 procedure comprises performing a secure hashing algorithm.

add

D **E**